



# Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 31 March 2004

Current Nationwide  
Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- The California ISO reports hot temperatures in Southern California are driving the demand for electricity to unusually high levels for this early in the year, necessitating a Stage One Electrical Emergency. (See item [2](#))
- The Oregonian reports federal authorities are investigating a scheme where thousands of illegal immigrants crossed into Oregon to fraudulently obtain driver's licenses, as well as key documents for gaining credit cards, opening bank accounts, and boarding airplanes. (See item [8](#))
- Reuters reports bomb threats against three U.S. passenger jets and two Amtrak trains triggered extensive security checks but no explosives were found. (See item [13](#))
- IDG News Service reports that Cisco Systems is warning customers about the public release of computer code that exploits multiple security vulnerabilities in Cisco products. (See item [27](#))

### DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

*March 30, Canadian Press* — **Deal will give TransCanada Power nine generating stations in North America. TransCanada Power LP has bought two U.S. power plants from TransCanada Corp. of Calgary in a deal worth US\$402.6-million. Under the agreement, TransCanada Power will acquire the ManChief power facility in Colorado and Curtis Palmer facility in New York.** Once the deal is completed, TransCanada Power will own nine power plants in Canada and the United States, with total generating capacity of 688 megawatts. "The ManChief and Curtis Palmer facilities are quality assets that complement our current generation portfolio," said Sean McMaster, TransCanada Power president. "This sale is consistent with our portfolio management strategy to divest mature assets and redeploy capital to allow TransCanada to pursue growth opportunities," said Hal Kvisle, TransCanada's CEO. Source: <http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/LAC/20040330/RTRANS30/TPBusiness/Canadian>

2. *March 29, California ISO* — **Heat wave sparks Stage One emergency. Hot temperatures in Southern California are driving the demand for electricity to unusually high levels for this early in the year, necessitating a Stage One Electrical Emergency which started at 1:50 p.m. on Monday, March 29.** The Stage One gives the California ISO additional authority to require power plants and transmission owners to respond to ISO instructions. "Temperatures are running about 10 degrees above forecast in Southern California," said Jim Detmers, Vice President for Operations at the California ISO. "We also had 770 megawatts of power plants trip out of service this morning. When outages coincide with high loads, we can quickly run out of options." The California ISO is a not-for-profit public benefit corporation charged with managing the flow of electricity along California's open-market wholesale power grid. Source: <http://www.caiso.com/docs/09003a6080/2f/23/09003a60802f234a.pdf>

[\[Return to top\]](#)

## **Chemical Sector**

3. *March 30, Occupational Safety & Health Administration* — **OSHA forms alliance with EPA and six chemical organizations.** Managing chemical reactivity hazards in the workplace received a major boost today, March 30, when the Environmental Protection Agency and six organizations involved in the chemical industry signed an Alliance with the Occupational Safety and Health Administration (OSHA). Joining OSHA and EPA in the Alliance are the American Chemistry Council, the American Institute for Chemical Engineers' Center for Chemical Process Safety, the Chlorine Institute, Inc., the Mary Kay O'Connor Center for Chemical Process Safety, the National Association of Chemical Distributors, and the Synthetic Organic Chemical Manufacturers Association. **The Alliance's goal is to offer a means for the group to provide information, guidance and access to training resources to their members, customers, contacts and others involved in the manufacture, distribution, use and storage of chemicals.** Working together, each organization will strive to provide chemical reactivity hazards management information, methods and tools to a variety of audiences while, at the same time, gain experience in the use of methods and tools to continuously improve identification and management of the hazards. Source: [http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_tabl e=NEWS\\_RELEASES&p\\_id=10762](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_tabl e=NEWS_RELEASES&p_id=10762)

## **Defense Industrial Base Sector**

4. *March 30, The Virginian–Pilot (VA)* — **Two more Navy jets crash. Two more jets crashed Monday, March 29, bringing to four the number of Navy aircraft lost in the past six days.** In each case, the pilots and crew ejected safely. Monday's accidents involved a Georgia–based F/A–18 Hornet that crashed in Tennessee and an F–14 Tomcat based at Oceana Naval Air Station that went into the ocean off Long Beach, CA. On Wednesday, March 24, a Beaufort, SC–based Hornet was lost off the South Carolina coast. On Friday, March 26, an Oceana–based Hornet burst into flames just before attempting to take off from Raleigh–Durham International Airport in North Carolina. The accidents have come without any explanation from officials, who said they are studying the incidents. The Navy has lost five aircraft, valued in excess of \$150 million, in March. Another F/A–18 crashed on March 10 at Lemoore Naval Air Station, CA, when the jet overturned while attempting to take off. **Often following such a rash of mishaps the Navy will order a safety stand down. As of Monday, March 20, no such orders had been issued, but it is possible officials are considering it,** said Mike Maus, a spokesperson for the Atlantic Fleet Naval Air Force in Norfolk, VA. Source: <http://home.hamptonroads.com/stories/story.cfm?story=68180&r an=15588>

5. *March 29, Aerospace Daily* — **Army plans expanded weapons tests on UAVs. U.S. Army researchers say they plan to expand the kinds of weapons fired in tests from unmanned aerial vehicles (UAVs). The use of armed Predator UAVs by non–Army U.S. forces in recent military operations has helped fuel the Army's interest in such platforms.** "Certainly, the weaponization of UAVs is a very hot and interesting topic right now, and we're doing some things along those lines, too," said Col. William Gavora, commander of the Army's Aviation Applied Technology Directorate (AATD), based at Fort Eustis, VA. The Army already has launched Brilliant Anti–armor (BAT) and Viper Strike munitions from the Hunter UAV in tests, and AATD plans to start shooting 70–millimeter rockets this summer from its Vigilante test bed, a small, unmanned rotorcraft, Gavora said. **The Vigilante tests will begin with Hydra 70 rockets and later move on to Advanced Precision Kill Weapon System (APKWS) rockets,** said Raymond Wall, chief of the directorate's systems integration division. Source: [http://www.aviationnow.com/avnow/news/channel\\_aerospacedaily\\_story.jsp?id=news/arm03294.xml](http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/arm03294.xml)

## **Banking and Finance Sector**

6. *March 30, Agence France–Presse* — **Virus creators run online credit card scam. Internet security experts on Monday, March 29, warned that the creators of some of the latest computer viruses were using computers infected by the bugs to run online scams to get credit card information from unsuspecting buyers. "There is an operation of fake online shops running on infected home computers, which are being controlled by hackers or criminals,"** said Mikko Hypponen, head of anti–virus research at Finland's F–Secure. Many

of the recent bugs open a so-called back door on infected computers, giving their creators access to the contaminated machines without the owners' knowledge. To avoid being traced, the Websites move from computer to computer, leaving buyers with no other real information than the Internet Protocol (IP) address of the infected machine that registered their credit card information. Many of the fraudulent Websites appear to be legitimate online software vendors, offering popular computer programs for a fraction of their real price, and often their services are advertised through spam messages, Hypponen said. The fact that the online fraudsters now use infected home computers to run their online rackets makes it significantly more difficult to track them down, analysts concluded.

Source: [http://sify.com/news\\_info/fullstory.php?id=13442609](http://sify.com/news_info/fullstory.php?id=13442609)

7. *March 30, The Press (NZ)* — **Scamsters target Westpac again.** Westpac customers in New Zealand have been hit with another e-mail scam which tries to trick them into revealing their precious security details. The bank's New Zealand media manager, Paul Gregory, confirmed that Westpac customers had been targeted by scamsters for at least the fourth time this year. The e-mail to the "valued customer" purports to be from Westpac and tells recipients the bank has just installed a new security system — ironically to keep fraud at bay and investments safe. "Due to this technical update we are insisting our clients verify to reactivate their accounts," the e-mail states. **About sixty Westpac customers had contacted the bank but only two had entered their details — less than on previous occasions,** Gregory said. "I wouldn't want to be too definite but it seems to us it has gone out to less people this time. That's our draft conclusion," he said. **However, it was becoming more difficult to detect a fraudulent Website from the real thing.**

Source: <http://www.stuff.co.nz/stuff/0,2106,2859680a13,00.html>

8. *March 28, The Oregonian* — **Feds uncover driver's license fraud operation. Thousands of illegal immigrants have crossed into Oregon to fraudulently obtain driver's licenses, key documents for gaining credit cards, opening bank accounts and boarding airplanes, federal authorities investigating the sophisticated scheme say. They say the operation, which was halted in 2003, is the biggest fraud and immigration case of its kind in Oregon.** "Thousands and thousands and thousands and thousands of people that should not be getting driver's licenses are," said Michael Williams, a special agent with U.S. Immigration and Customs Enforcement and a lead investigator on the case. The investigation centers on three Washington County, OR, brothers who operated driving and testing schools and a Southeast Portland man who recruited illegal immigrants from New York. In January, a woman was convicted of selling counterfeit mail as part of the scheme. The bogus mail was used to falsely prove residency to Oregon Driver and Motor Vehicle Services clerks. Three factors led to the operation's success in Oregon: 1) the state issues licenses based on residency, not immigration status. 2) until this year, DMV accepted personal mail as proof of residency at a specific Oregon address, and 3) DMV officials didn't enforce the agency's rules.

Source: [http://www.oregonlive.com/news/oregonian/index.ssf?/base/fro nt\\_page/1080392900239921.xml](http://www.oregonlive.com/news/oregonian/index.ssf?/base/fro nt_page/1080392900239921.xml)

[\[Return to top\]](#)

## **Transportation Sector**

9. *March 30, Department of Transportation* — **Secretary Mineta announces \$90.8 million for Boston–Logan International Airport.** U.S. Transportation Secretary Norman Y. Mineta announced a federal commitment of \$90.8 million for construction of a new runway and other projects at Boston–Logan International Airport that will allow the airport to reduce flight delays. **Secretary Mineta said. “Air travel is an engine of economic growth, and this investment will gear up Boston to tap into the resurgence of air travel.”** The money comes through a "letter of intent" (LOI) signed with the U.S. Department of Transportation's Federal Aviation Administration (FAA) and the Massachusetts Port Authority (Massport). Under the LOI, the FAA will provide funding to Massport for the project between fiscal years 2005 and 2012.  
Source: <http://www.dot.gov/affairs/dot04204.htm>
10. *March 30, Reuters* — **Supreme Court allows border search of gas tanks. A unanimous U.S. Supreme Court ruled on Tuesday, March 30, that agents at the border can take apart and search a vehicle's gas tank for drugs or contraband without violating constitutional privacy rights.** In a victory for the U.S. Justice Department, which argued routine searches can catch drug smugglers and terrorists, the high court said agents need not have a reasonable suspicion the gas tank contained illegal items. The justices overturned a U.S. appeals court ruling that such inspections violated the constitutional guarantee against unreasonable searches and seizures of evidence. The decision, written by Chief Justice William Rehnquist, reaffirmed the broad power of customs agents to conduct searches at the border, even if they do not have a specific reason to suspect wrongdoing.  
Source: <http://www.reuters.com/newsArticle.jhtml;jsessionid=ZVJK40ZUDTQO4CRBAEOCFEY?type=domesticNews&storyID=4701338>
11. *March 30, The Trucker* — **NTSB head praises FMCSA for HOS, but says they must be enforced.** National Transportation Safety Board (NTSB) Chairman Ellen Engleman–Connors on March 29 praised the new Hours of Service (HOS) rules and the Federal Motor Carrier Safety Administration (FMCSA), saying that the rules reduce fatigue by limiting drivers' hours of duty. She made the comments in connection with the start of National Sleep Awareness Week, which began March 29 and continues through April 4. **But Engleman–Connors said there is still much to be done, noting that some of the NTSB's safety recommendations still need to be carried out in other transportation modes so that "all vehicle operators receive enough rest."** According to an NTSB release, fatigue and hours of work have been on NTSB's "most wanted" list since 1990 but haven't been implemented by the applicable federal agencies.  
Source: [http://www.thetrucker.com/stories/03\\_04/0330\\_ntsb\\_hos.html](http://www.thetrucker.com/stories/03_04/0330_ntsb_hos.html)
12. *March 30, Bloomberg* — **Canada airport, passport vetting is lax, auditor says.** Canadian screening for terrorists or criminals posing as airport workers or using fake documents such as passports still has “serious” flaws two years into a C\$7.7 billion (US\$5.89 billion) program to improve security, the government's auditor said. **Federal police still match fingerprints against a criminal database by hand, border agents don't get information on lost or stolen passports and airport baggage handlers aren't checked for possible ties to criminal groups, Auditor General Sheila Fraser said in a report in Ottawa.** “These matters are serious and need to be addressed,” Fraser said. The lists used to screen tourists and refugees coming to Canada “are in disarray,” she said. The government is addressing some of the issues raised by the auditor general. Canada's passport office reached an agreement in principle to link

its information on lost or stolen documents with federal police.

Source: <http://quote.bloomberg.com/apps/news?pid=10000082&sid=aaRS27KBx0A4&refer=canada>

13. *March 30, Reuters* — **Jets, trains targeted with bomb threats. Bomb threats against three U.S. passenger jets and two Amtrak trains triggered extensive security checks Tuesday, March 30, but no explosives were found, authorities said.** Security officials, aided in some cases by sniffer dogs, took hours to sweep through the planes operated by Northwest Airlines. But the searches, of passengers and luggage as well as the airliners themselves, ended without incident. “Fortunately these threats turned out not to be credible,” said Yolanda Clark of the Transportation Security Administration. **There were also bomb threats against two Amtrak trains traveling between New York and Miami.** A spokesman for the railroad said more than 140 passengers were taken off the northbound Palmetto at the Selma–Smithfield station in North Carolina and the train was searched. Service resumed after a delay of nearly 2 1/2 hours. At roughly the same time, 176 passengers were evacuated from the Silver Meteor in Philadelphia. Service resumed after a 45–minute delay. Nothing was found on either train, said Amtrak spokesman Dan Stessel. Security officials aided by sniffer dogs swept through three U.S. passenger jets Tuesday after they were targeted by bomb threats, authorities said.

Source: <http://msnbc.msn.com/id/4632410/>

14. *March 29, Department of Transportation* — **DOT provides \$13.2 million for Connecticut I–95 repairs.** U.S. Transportation Secretary Norman Y. Mineta today, March 29, made available \$13.2 million to Connecticut for I–95 recovery and repair. The relief money is being released in the wake of last Thursday’s truck accident in Bridgeport, CT. The funds will come from two sources. The Department will provide \$2 million in emergency relief funds to the state. In addition, Connecticut will be allowed to redirect \$11.2 million in federal highway funds to be used for bridge repair and recovery. **“I–95 is crucial to Connecticut, the Northeast and the country and that is why it is so important to the President and me that we invest in keeping America’s economy moving,” said Secretary Mineta.** The funds made available today will help state and local officials pay for the repairs underway on the I–95 bridge in Bridgeport damaged in last week’s truck accident. The money can be used to reimburse first responders and offset related costs such as detours, extra train service, public information systems, traffic controls and other accident–related measures.

Source: <http://www.dot.gov/affairs/fhwa204.htm>

[[Return to top](#)]

## **Postal and Shipping Sector**

15. *March 30, Congress Daily* — **Lawmakers begin drafting postal overhaul legislation.** Now that the House Government Reform Committee has wrapped up its postal overhaul hearings, and with only one more hearing planned in the Senate Governmental Affairs Committee, lawmakers have begun drafting legislation to change the U.S. Postal Service. Senate Governmental Affairs Committee Chairwoman Susan Collins, R–Maine, will introduce legislation with Sen. Thomas Carper, D–Delaware, at the end of April. Rather than introducing companion legislation in the House, House Government Reform Committee Chairman Tom Davis, R–Virginia, plans to introduce his own bill with Rep. John McHugh, R–New York,

chair of the House committee's postal panel. **As lawmakers put these bills together, the most hotly debated topics probably will be workforce issues, such as reducing the size of the postal workforce and opening employee health benefits to collective bargaining.** Collins also has said she intends to change the postal worker compensation system. **Other potentially contentious issues include scaling back the number of mail distribution centers and determining the Postal Service's ability to compete with private-sector mailers.**

Source: <http://www.govexec.com/dailyfed/0304/033004cdam1.htm>

16. *March 30, Reuters* — **FedEx's China sales.** FedEx Corp. increased revenues in China by an annual 40 percent in the quarter ending in February, but said again it was battling on an uneven playing field. **FedEx which does not normally divulge sales by country or region, fears government legislation now in the works could impede progress and protect China's postal monopoly.** FedEx is vying with Deutsche Post's DHL Express and United Parcel Service Inc. to muscle in on an insular sector that it says could one day be the world's top cargo market. Rocketing trade, which surpassed \$850 billion last year, is driving Chinese demand for air freight, although the market is now dominated by local monopoly China Post and domestic freight forwarders such as Sinotrans Ltd. **Now Beijing is drafting rules to tax foreign courier firms to help it fund a rural postal service, industry insiders say.** UPS which has 18 percent of the Chinese market, has said sales there could have climbed 50 percent to \$300 million in 2003. Analysts estimate the market could be worth \$1.5 billion annually. **Despite loosening regulations since China joined the World Trade Organization, analysts say the most lucrative areas will continue to be off-limits to foreign couriers.** Last September, Beijing allowed foreign companies to deliver some documents from China abroad but barred them from personal letters and most government mail.

Source: [http://money.cnn.com/2004/03/30/news/international/fedex\\_chi\\_na.reut/](http://money.cnn.com/2004/03/30/news/international/fedex_chi_na.reut/)

[[Return to top](#)]

## **Agriculture Sector**

17. *March 30, Canadian Press* — **Avian flu possibly found outside hot zone.** Canadian officials are checking out concerns that avian flu has been detected on a chicken farm outside a hot zone where hundreds of thousands of poultry will be slaughtered. Chickens on the farm, located in the Fraser Valley, exhibited signs of a common illness called Newcastle Disease, but also showed possible avian flu symptoms. The farm was placed under quarantine, the first outside a so-called hot zone around an Abbotsford-area poultry farm where the virus was first detected.

Source: <http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/LAC/20040330/NATS30N/TPNational/Canada>

18. *March 30, Tennessean* — **Testing horse show bioterrorism preparation.** The Tennessee Department of Agriculture will test local, state, and federal responses to a simulated act of bioterrorism at a major horse show. The exercise will take place in Shelbyville, home of the Tennessee Walking Horse National Celebration, an equine event that attracts tens of thousands of spectators and hundreds of horses every summer. "Basically, this is a way that we can test the various agencies to see how we would respond if something did happen," said Tom Womack, spokesman for the department. More than 100 people, including veterinarians, police,

emergency medical workers, and horse owners, are expected to attend the event. "This is a table-top discussion only, there's no field exercise. The scenario will be read and the different groups will respond with what should be done, Womack said. **He declined to say what agent will be introduced to the horse show as part of the simulation, but he said it would be harmful, if not deadly, to horses and would cause humans to react with flulike symptoms.** "It's something that would have an immediate impact," he said.

Source: <http://www.tennessean.com/local/archives/04/03/49048403.shtm>  
[l?Element\\_ID=49048403](#)

19. *March 30, Kansas State University* — **Kansas State uses geographic tools to track plant pathogens.** The Asian soybean aphid, native to China, Korea, and Japan, has invaded the United States. It was identified as a new crop pest on the North American continent in 2000, after appearing simultaneously in 11 states. It was probably carried in accidentally, says Sonny Ramaswamy, Kansas State University entomology department head. **He sees the aphid invasion as a training exercise for scientists to prepare for an agroterrorist strike that pits a foreign insect pest against U.S. crops.** "In fact, insects, including this aphid, are natural carriers and vectors of a lot of plant pathogens. When I heard about the aphid, I realized we could learn a lot if we studied this outbreak as if it were a deliberate introduction," Ramaswamy said. "We were tackling a complex puzzle: we wanted to see if we could determine how fast the aphid moves, where it's been; then if we could predict where it's going throughout the country, and, finally, by looking at the data could we work backwards to determine its point of entry," Ramaswamy said. **GIS showed how the aphid moved across the country, the topographic and environmental characteristics favoring its dispersal, and where the aphid could go next. GIS analysis points to Cook County, IL, as the point of entry.**

Source: [http://www.eurekalert.org/pub\\_releases/2004-03/ksu-kug031904.php](http://www.eurekalert.org/pub_releases/2004-03/ksu-kug031904.php)

[[Return to top](#)]

## **Food Sector**

20. *March 29, MSNBC* — **Seven labs chosen to test for mad cow.** Seven public state laboratories across the nation have been chosen to conduct testing for mad cow disease, the fatal brain disease that first showed up in the United States in December, the U.S. Department of Agriculture (USDA) said Monday, March 29. **The labs are spread out from New York to California and will be responsible for checking samples of cattle brains from all 50 states for bovine spongiform encephalopathy.** Currently, that task is handled by a single facility, the USDA's National Veterinary Services Laboratory in Ames, IA, which will coordinate national efforts and confirm any initial positives.

Source: <http://msnbc.msn.com/id/4626203/>

21. *March 29, just-food.com* — **Potato salad recalled. Grocery store chain BI-LO has recalled a batch of potato salad products after listeria bacteria were found in routine testing.** Vince's Famous Southern Style Potato Salad, distributed through BI-LO stores, has been removed from sale after a sample taken by the Tennessee Department of Agriculture from a BI-LO store in Chattanooga revealed a positive reading for listeria. Listeria bacteria can cause sickness and can be particularly serious in infants, the elderly, pregnant women, and individuals with a weak immune system. The company said no cases of illness related to the product have

been reported.

Source: [http://www.just-food.com/news\\_detail.asp?art=57116](http://www.just-food.com/news_detail.asp?art=57116)

[\[Return to top\]](#)

## **Water Sector**

22. *March 30, Gannett News Service* — **Nuclear sites put drinking water sources at risk. Major sources of drinking water remain at risk of serious contamination from the nation's nuclear weapons complexes, despite billions in federal spending to clean up hazardous waste produced at these sites, according to a new report.** The seepage of radioactive and toxic byproducts into vital water resources pose grave health dangers to the tens of thousands of workers at these nuclear facilities, area residents, and people who live dozens of miles away, authors of the report concluded. "There is an extremely serious risk around sites where there is a lot of waste and groundwater," said Arjun Makhijani, president of the Institute for Energy and Environmental Research, which released the report Monday, March 29. Among the major water bodies facing the greatest threat are the Columbia River in Washington, the Clinch River in Tennessee, the Great Miami River in Ohio and the Savannah River in South Carolina, the alliance said. Ohio's Great Miami Aquifer, the Ogallala Aquifer in Texas, and Idaho's Snake River Aquifer are among the underground water sources being polluted, the report said. **Kingston, TN Richland, WA, and Cincinnati, OH, are among the cities that rely almost exclusively on at-risk aquifers or rivers for drinking water.**

Source: [http://www.usatoday.com/news/washington/2004-03-29-nuclear-g ns\\_x.htm](http://www.usatoday.com/news/washington/2004-03-29-nuclear-g ns_x.htm)

[\[Return to top\]](#)

## **Public Health Sector**

23. *March 30, New Kerala (India)* — **Scientists invent fast new test for TB. An Italian research team has come up with a new fast test for diagnosing tuberculosis, a disease that still infects a third of the world's population, reports Xinhua.** The new method has been invented and patented by Rome's Spallanzani Hospital, which specializes in rare and infectious diseases, the Italian media reported. **According to medical experts, the importance of the new test method is two-fold in that it not only enables doctors to distinguish latent and active forms of the disease in just two days, but also allows them to gauge the efficacy of the therapy in patients with the active form of the disease.** Each year there are some three million TB-linked deaths in the world. The ability to quickly and accurately detect the infection, experts say, is crucial for overall control of tuberculosis.

Source: <http://www.newkerala.com/news-daily/news/features.php?action =fullnews&id=8067>

[\[Return to top\]](#)

## **Government Sector**

24. *March 30, General Accounting Office* — **GAO-04-160: Improved Planning Needed to Ensure Delivery of Essential Government Services (Report published in February).** To

ensure that essential government services are available in emergencies — such as terrorist attacks, severe weather, or building-level emergencies — federal agencies are required to develop continuity of operations (COOP) plans. Responsibility for formulating guidance on these plans and for assessing executive branch COOP capabilities lies with the Federal Emergency Management Agency (FEMA), under the Department of Homeland Security. FEMA guidance, Federal Preparedness Circular (FPC) 65 (July 1999), provides elements of a viable COOP capability, including the requirement that agencies identify their essential functions. **GAO was asked to determine the extent to which (1) major civilian executive branch agencies have identified their essential functions and (2) these agencies' COOP plans follow FEMA guidance. To ensure that the executive branch can provide essential services during emergencies, GAO recommends, among other things, that the Secretary of Homeland Security take steps to improve agency COOP plans and FEMA's process for assessing these plans.** In commenting on a draft of this report, the Under Secretary for Emergency Preparedness and Response agreed that FEMA could do more to improve COOP planning, and that FEMA has begun making such improvements. Highlights:

<http://www.gao.gov/highlights/d04160high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-160>

[[Return to top](#)]

## **Emergency Services Sector**

### **25. *March 30, AccessNorthGa (Gainesville, GA)* — Forsyth 'Reverse 911' up and running.**

Forsyth County's Reverse 911 system is now operational, according to Sheriff Ted Paxton. **Paxton says Reverse 911 is a computerized system that allows the Sheriff's Office to notify homes in a specific area by telephone in case of an emergency. The system will dial selected numbers and a pre-recorded message will be played when someone answers.** "Reverse 911 greatly enhances our ability to serve the county," Paxton says. "Examples of where we might utilize it would be in the event of a toxic chemical spill or fire where immediate evacuation would be needed." Another feature of the system is the "Guardian Project." Paxton says that portion of the system allows homebound residents to be contacted by phone once a day, to check up on their welfare.

Source: <http://www.accessnorthga.com/news/hall/newfullstory.asp?ID=8.0249>

### **26. *March 29, Firehouse.com* — FDNY will train to cope with terror. Counterterrorism training will be the FDNY's top priority for the next two years, according to a landmark plan prompted by the September 11 attacks and slated for release today, March 29.**

Hundreds more firefighters and medics will be trained to handle hazardous materials, a database of potential terrorist targets will be created and the department will hold monthly terrorism training exercises, according to the plan, obtained by the Daily News. Among the recommendations: Train 25 ladder companies and 25 medic crews to respond to chemical, biological and nuclear attacks, bumping to roughly 1,000 the number of FDNY workers capable of handling hazardous materials. Create a database listing 150 potential terror targets citywide. Conduct regular training sessions in conjunction with NYPD and Port Authority cops, as well as workers from hospitals and utilities.

Source: <http://www6.lexisnexis.com/wpublisher/EndUser?Action=UserDisplayFullDocument&orgId=34&topicId=17906&docId=1:84059107&start=1>

## **Information and Telecommunications Sector**

27. *March 29, IDG News Service* — **Cisco warns of new hacking tool kit.** Cisco Systems Inc. has warned customers about the public release of computer code that exploits multiple security vulnerabilities in Cisco products. **Using exploits for nine software vulnerabilities, the program could allow malicious hackers to compromise Cisco's Catalyst switches or a wide variety of machines running versions of the company's Internetwork Operating System (IOS).** Called the Cisco Global Exploiter, the program appears to give users a menu of choices, depending on the system they are trying to crack. It offers, for example, the "Cisco 677/678 Telnet Buffer Overflow Vulnerability" or the "Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability," according to the Web site, [www.kotik.com](http://www.kotik.com). Computer code for a program matching the description in the Cisco security notice was posted on the French-language computer security exploit site yesterday. While many of the exploits can be used only to shut down affected Cisco devices in denial-of-service attacks, at least one enables remote attackers to run malicious code on the affected system without needing a username or password, according to the Cisco security notice. Customers should patch software vulnerabilities exploited by the program.  
Source: <http://www.computerworld.com/securitytopics/security/story/0,10801,91748,00.html>

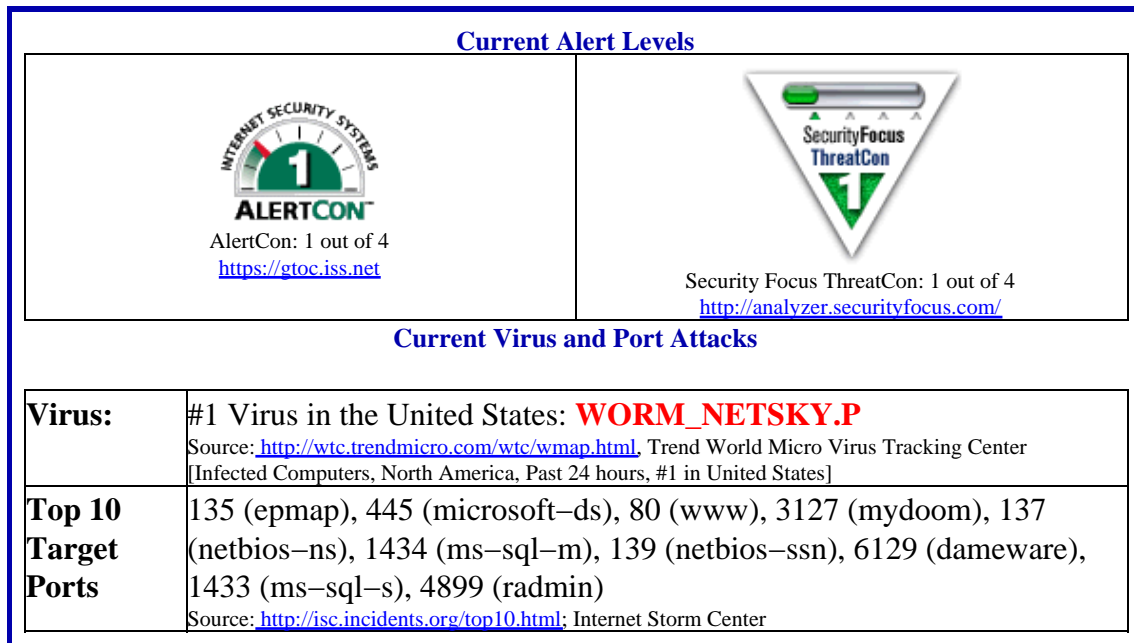
28. *March 29, CNET News* — **NetSky variant a greater threat than thought.** Security company Symantec raised its severity rating of the latest incarnation of the NetSky worm. NetSky.Q was upgraded from a level 2 to level 3 threat on the security firm's five-point rating system. The company said it has received 379 reports of the worm since its discovery Sunday, March 28. NetSky is a mass-mailing worm that uses a bogus sender address and continually changes its subject line and content. An e-mail attachment usually carries an .exe, .pif, .scr or .zip file extension. The worm distributes itself to e-mail addresses in a victim's hard drive and copies itself into shared folders via file-sharing programs. **NetSky.Q is expected to release a denial-of-service attack between April 8 and April 11 on several Websites, including those of eDonkey2000, Kazaa, eMule, Cracks.am and Cracks.st,** according to Symantec.  
Source: <http://news.com.com/2100-7355-5181476.html?tag=nl>

29. *March 26, eSecurity Planet* — **RealNetworks confirms buffer overflow problem.** Digital media delivery firm RealNetworks confirmed a buffer overflow vulnerability in its Helix Universal Server product, warning that a root exploit could give an attacker "inappropriate access" to compromised system. RealNetworks first warned of the flaw in January, describing it as a simple denial-of-service issue, but on Friday, March 26, the company released an updated advisory Friday to confirm the existence of a "potential root exploit." A root exploit could give an attacker complete control over a susceptible machine to execute malicious code. **On Windows platforms where the Helix Server is run as an NT Service, the bug could allow arbitrary code execution under the context of the NT SYSTEM account.** Vulnerable products includes Real's Helix Universal Mobile Server & Gateway 10, version 10.1.1.120 and prior and the Helix Universal Server and Gateway 9, version 9.0.2.881 and prior. RealNetworks has released an updated version of the Helix Universal Server or Gateway:  
<http://service.real.com/help/faq/security/security022604.htm>

Source: <http://www.esecurityplanet.com/prodser/article.php/3332201>

30. *March 15, General Accounting Office* — **GAO-04-354: Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems (Report)**. Computerized control systems perform vital functions across many of our nation's critical infrastructures. For example, in natural gas distribution, they can monitor and control the pressure and flow of gas through pipelines. In October 1997, the President's Commission on Critical Infrastructure Protection emphasized the increasing vulnerability of control systems to cyber attacks. The House Committee on Government Reform and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census asked GAO to report on potential cyber vulnerabilities, focusing on (1) significant cybersecurity risks associated with control systems (2) potential and reported cyber attacks against these systems (3) key challenges to securing control systems and (4) efforts to strengthen the cybersecurity of control systems. **GAO recommends that the Secretary of the Department of Homeland Security (DHS) develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems.** DHS concurred with GAO's recommendation. Highlights: <http://www.gao.gov/highlights/d04354high.pdf>  
Source: <http://www.gao.gov/new.items/d04354.pdf>

### Internet Alert Dashboard



[[Return to top](#)]

## General Sector

31. *March 30, Bloomberg* — **UK arrests eight terrorism suspects**. London police said Tuesday, March 30, they seized more than a half ton of ammonium nitrate fertilizer, which can be used to make a bomb, and arrested eight men suspected of planning a terrorist attack. Raids were made

at 24 locations in and around London in an operation at dawn involving 700 officers from five police forces, Peter Clarke, head of the Anti-Terrorist Branch of London's Metropolitan Police, said. **Some of the sites are near London's Heathrow, Gatwick and Luton airports, and another is on the main route to Stansted airport.** "The men who have been arrested are all British citizens...aged between 17 and 32," Clarke said. Sir John Stevens, head of the London police force, has said a terrorist attack on London is "inevitable" and that the bomb attacks in Madrid, which have been linked to al-Qaeda, should act as a "wake-up call" to Britain and Europe. **Fertilizer has been used in bomb attacks on New York's World Trade Center in 1993, in Oklahoma City in 1995, London's Canary Wharf building in 1996, and the Indonesian resort of Bali in 2002.**

Source: <http://quote.bloomberg.com/apps/news?pid=10000102&sid=a7qTyCWskPgE&refer=uk>

32. *March 30, Reuters* — **Philippines says foils major attack.** The Philippines said Tuesday, March 30, that it has foiled a "Madrid-level" terror attack on shops and trains in the capital Manila by arresting four suspected Islamic militants and seizing a large amount of explosives. **The suspected plot by members of the Abu Sayyaf group comes as campaigning heats up ahead of May 10 national elections in which President Gloria Macapagal Arroyo, a firm ally in the U.S.-led war on terror, is seeking a new term.** Police intelligence chief Ismael Rafanan said the arrested leader of the cell was the cousin of Abu Sayyaf leader Khaddafy Janjalani. The cousin is suspected of beheading U.S. citizen Guillermo Sobero after he was kidnapped in 2001. Defense Secretary Eduardo Ermita told reporters **the arrests followed a tip-off, and one of the suspects had been trained by the al Qaeda-linked Jemaah Islamiah (JI) to handle explosives.** The JI has been blamed for several bomb blasts in Manila in December 2000, including one on a train, that killed 22 people. The 300-strong Abu Sayyaf group, based on an island chain southwest of southern Mindanao island, has been linked to al Qaeda, although many analysts say it has become a criminal gang.

Source: <http://uk.news.yahoo.com/040330/325/epurs.html>

33. *March 30, Associated Press* — **Statue of Liberty to reopen this summer.** The Statue of Liberty, closed immediately after the September 11 terrorist attacks, will reopen to the public this summer, officials said Tuesday, March 30. Pledges of \$7 million in donations will finance upgrades that were necessary at the national monument before it could be reopened. Currently, tourists can visit Liberty Island but are not allowed inside the statue in New York Harbor. "Safety of our citizens and preservation of the statue are our main goals," said Secretary of the Interior Gail Norton, acknowledging that the 118-year-old statue was "an attractive terrorist target." According to Norton, an examination of the national monument revealed potential for fire problems and a lack of exits. **Screening procedures, much like those at airports, and a reservation system to reduce long lines will be implemented once the monument reopens in late July,** Norton said. She said after the upgrades are completed, the public will be allowed to climb the 354 steps to the statue's crown, or observation deck.

Source: [http://www.cbsnews.com/stories/2004/03/30/national/main60935\\_2.shtml](http://www.cbsnews.com/stories/2004/03/30/national/main60935_2.shtml)

[[Return to top](#)]

## **DHS/IAIP Products &Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

**DHS/IAIP Warnings** – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

**DHS/IAIP Publications** – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

**DHS/IAIP Daily Reports Archive** – Access past DHS/IAIP Daily Open Source Infrastructure Reports

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions: [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 883-3644

Subscription and Distribution Information Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at (703) 883-3644 for more information.

### **Contact DHS/IAIP**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [info@us-cert.gov](mailto:info@us-cert.gov) or visit their Web page at [www.uscert.gov](http://www.uscert.gov).

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.